Regulation n°116

PROTECTION AGAINST UNAUTHORIZED USE

GRSG/Task-Force on KEY DEFINITION

GRSG-119 / October 2020

Status / Meeting Attendance

- 3rd Task-force WebMeeting, 28th September 2020:
  EC, NL, UK, DE, FR, JP, KR, CN, IN, OICA, CLEPA
- Follow up of 2nd Task-force WebMeeting, 26th June 2020:
  EC, UK, DE, OICA, CLEPA
- 2nd Task-force WebMeeting, 18th May 2020:
  EC, NL, DE, FR, OICA, CLEPA
- 1st Task-force F2F, Brussels, 18th Feb. 2020:
  EC, NL, UK, DE, FR, OICA, CLEPA

Status, Agreements within Task-Force

- Name of the new technology: “Digital Key”
- Other remote items, not referred to in UN ECE R116, e.g. power window, heating, are out of scope of R116 and out of scope of Task-Force discussions
- Risk of Relay attacks. The protocol used for smart device keys does not increase the risk for relay attacks. Not to be addressed with changes for digital key in the Task-Force.
- Digital Keys should not be possible to copy a digital key from ones smart device to another smart device (No duplication). The process preventing this is the pairing process. This process is not defined in UN R116 for traditional keys. For Digital Keys the manufacturer will provide documentation how this process works per Annex 11 (Revocation Process).
  - The OEM is responsible that the paired key only works with the vehicle it is paired with. Whether or not the “APP”/Software remains on an device, when the digital key is no longer paired is not OEM responsibility. (Revocation Process)
  - Unsafe smart device. It is possible to un-pair the key from the vehicle. (Revocation Process).
- Limitation of Key. The numbers of existing keys is not restricted by UN R116.
- Key Codification. Demonstrated by Cyber Security for Digital Key.

Status, Open Items – Work ongoing

- **Definition of the key:** Agreement that the definition must be updated for Digital Key. Agreement that the difference between Mechanical Key (physical key fob), Electronic Key (key card, integrated in key fob) and Digital Key (electronic solution possible to be installed on different devices incl. non OEM devices) must be clear. Missing: New draft text (to be provided for TF#4)
- **Cyber Security:** Per GRVA members risk of the connection is part of UN R155 risk assessment and risk mitigation plan. Written outcome of the discussions between the Chairs (GRSG/IWG Cybersecurity) is awaited.
- **Area of Operation of the key:** Diverse Position, OICA: Not defined for traditional devices. CPs: Must be restricted. Compromise tabled for TF#3, was not discussed.
- **Information to Vehicle Owner:** Agreement in TF#1 Annex 1 to clearly state a requirement that Revocation process and Authorization process must be provided to the vehicle owner. Text to be drafted.
- **Limitation of Key:** Agreement that a revocation process needs to be in place for digital key. Diverse Position: OICA: Documentation sufficient. CPs: Validity and revoking need further constraints. Proposed Compromise: Repeat requirement of paragraph 5.4 explicitly for revocation of key: “Deactivation of a digital key shall not result in an unsafe condition.” in Annex 11 for digital key.

Next Steps

Doodle ongoing for two further Task-Force meetings

- #4: between 2nd and 12th Nov. 2020
- #5: between 2nd and 12th Dec. 2020

Task: Finalize a working document for GRSG-120

Please participate and provide your inputs to the task force.

Thank you.